



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/045,893	01/12/2002	Koteshwerrao Adusumilli	42390P12318X	3131

⁷⁵⁹⁰
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1030

EXAMINER

BROWN, CHRISTOPHER J

ART UNIT	PAPER NUMBER
----------	--------------

2439

MAIL DATE	DELIVERY MODE
-----------	---------------

04/15/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/045,893
Filing Date: January 12, 2002
Appellant(s): ADUSUMILLI, KOTESHWERRAO

Brent Vecchia
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 3/11/2010 appealing from the Office action mailed 8/25/08.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The following are the related appeals, interferences, and judicial proceedings known to the examiner which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal:

Application 10/000154 is under appeal and is a parent to the present application.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

7099284	HALME	8-2006
6571221	STEWART	5-2003
20020099957	KRAMER	7-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 33-36, 38, 40, 42, 43, 45, 48, 50, 51, 52, and 54-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart US 6,571,221 in view of Kramer US 2002/0099957 in view of Halme 7,099,284.

As per claims 33, 42, 50, 56, and 59 Stewart teaches an interface to receive data from at least one wired client device and one wireless client device, (Col 8 lines 47-55). Stewart teaches logic to determine if the device is wired or wireless, (Col 7 lines 43-62, Col 8 lines 20-30). Stewart teaches requesting a secure connection from a wired or wireless device, (Col 13 lines 33-43). Stewart teaches that the client is authenticated in establishing a connection with the wired or wireless device, (Col 14 lines 29-44). Stewart does not teach SSL, WTLS or converting encrypted data to an unencrypted format.

Kramer teaches a security format conversion system including from SSL, TLS, [0024], [0050]. Kramer teaches converting the encrypted data to a different format (encryption/decryption) [0050]. Kramer teaches a network interface and a server to receive converted data, [0049]. It is well known in the art that the port used and key exchanged in SSL, and TLS indicate the recipient decrypt the encrypted data. It would have been obvious to one of ordinary skill in the art to use the protocols of Kramer with the system of Stewart because SSL and TLS are widely accepted and compatible protocols.

Halme teaches using a VPN protocol where encrypted data is sent from one private network over a public network to a second private where it is decrypted at a node and forwarded over a private network (data center) (Col 1 lines 20-35, Col 3 lines 35-55, Fig 3). It is well known in the art that SSL is used with VPN protocol. It is well known that LANs may contain multiple clients and servers. It would have been obvious to one of ordinary skill in the art to use the VPN of Halme with the previous combination because it allows end to end security.

As per claim 34, Stewart teaches that the device has an interface to transmit data and to receive data from a server, (Col 14 lines 16-22).

As per claims 38, 45, and 52, Stewart teaches requesting a digital certificate of the client and authenticating that certificate, (Col 14 lines 19-22, 29-33).

As per claims 35, 36, 40, 43, 48, 51, 54, and 55 Stewart does not teach protocols or determining the client type dependent on protocol.

Kramer teaches a security format conversion system including from SSL or WTLS, [0050].

As per claims 57, and 58 Kramer teaches that all decryption takes place in a VPN server or firewall, which is located between a public network and a data center server, [0049], Fig 3.

Claims 37, 41, 44, 46, and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart US 6,571,221 in view of Kramer US 2002/0099957 in view of Halme 7,099,284 in view of Douglas US 2004/0010684.

As per claims 37 and 44, Stewart fails to teach sending a certificate from the server to the client.

Douglas teaches a handshaking technique where the client and server exchange certifications and digital signatures to authenticate each other, [0031], [0032].

It would have been obvious to one of ordinary skill in the art to use the handshaking technique of Douglas with the system of Stewart-Kramer- Halme because it allows the client to authenticate the server thus ensuring that the client is not communicating with an unauthorized party.

As per claims 41, and 49, Stewart-Kramer-Halme fails to teach receiving a digital signature from the client device and validating said signature.

Douglas teaches a handshaking technique where the client and server exchange certifications and digital signatures to authenticate each other, [0029], [0030] [0031].

It would have been obvious to one of ordinary skill in the art to use the digital signatures of Douglas with the system of Stewart in order to confirm that data had not been manipulated in transit.

As per claim 46, Stewart –Kramer-Halme fails to teach verifying the validity period of the certificate.

Douglas teaches including a timestamp in the signed message, and validating said message, [0028], [0029]. It would have been obvious to one of ordinary skill in the art to use the timestamp of Douglas with the certificate of Stewart because it would prevent replay attacks [Douglas 0028].

Claims 39, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart US 6,571,221 in view of Kramer US 2002/0099957 in view of Halme 7,099,284 in view of Hajmiragha US 6,289,460

As per claims 39, and 47, Stewart-Kramer- Halme does not teach using a URL with a digital certificate.

Hajmiragha teaches sending a link, rather than the actual digital certificate, (Col 4 lines 40-43).

It would have been obvious to one of ordinary skill in the art to use the system of Stewart with the link of Hajmiragha, because the link prevents interception and modification of a digital certificate between parties.

Claims 53 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart US 6,571,221 in view of Kramer US 2002/0099957 in view of Halme 7,099,284 in view of Stubblebine US 6,216,231

As per claim 53, Stewart-Kramer- Halme does not teach updating a short lived server certificate based on a user defined interval.

Stubblebine teaches updating a short lived server certificate based on a user defined interval, (Col 15 lines 25-36).

It would have been obvious to one of ordinary skill in the art to use the updating certificates of Stubblebine with the Stewart-Kramer-Halme combination because short lived certificates increase security.

Claim 60 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart US 6,571,221 in view of Kramer US 2002/0099957 in view of Halme 7,099,284 in view of Bacha US 6,931,526

As per claim 60, the previous combination of Stewart, Kramer and Halme teaches SSL protocol, but not certificate revocation lists.

Bacha teaches authentication of certificates through SSL (a well known certificate exchange method) and if the session is new, comparing the SSL certificate to certificate revocation lists (col 10 lines 48-64)

It would have been obvious to one of ordinary skill in the art to use the CRL of Bacha with the SSL method as taught by the previous combination because it enhances security by checking the certificate against well known invalid certificates.

(10) Response to Argument

Appellant argues that Stewart does not disclose logic to convert SSL and WTLS encrypted data to unencrypted formats. Examiner admits that Stewart does not teach said protocols, and does not rely on Stewart to teach SSL and WTLS. Examiner merely relies on Stewart to teach a hybrid interface that accepts both wired and wireless communications. Kramer is relied upon to teach SSL and WTLS.

Appellant argues that Stewart does not render obvious that an apparatus resides in a data center couple between a public network and a server of the data center. Examiner does not rely on Stewart for said teaching. However the examiner has met this limitation through Kramer and Halme.

Appellant argues that Stewart does not teach the hybrid wired and wireless access point because it is in front of instead of behind, a centralized network. While the examiner relies on

Stewart to teach such an interface, Kramer teaches that the interface is behind the centralized network rather than in front of it.

Appellant argues that Kramer does not teach A) VPN access server does not have logic to convert SSL encrypted data, and WTLS encrypted data, B) that VPN access server 314 receives WTLS data, C) that conversion typically takes place at a WAP gateway, and D) an apparatus to reside in a data center coupled between a public network and a server of the data center.

Examiner argues that Kramer teaches that a VPN or proxy server that does have logic to decrypt SSL and WTLS data. It is well known in the art that a Virtual Private Network is to secure a communication from a client to a VPN server where the data is decrypted. Kramer teaches in [0049], and [0050], that the VPN is a secure connection between the server and an external client outside of the private corporate network. Although the external client establishes the connection, Kramer teaches that VPN server has software and hardware to facilitate the connection at VPN server 314, or Proxy Server 312. Kramer teaches that security for the connection may be SSL protocol or WTLS protocol encryption/decryptions. It would have been understood by those of ordinary skill in the art that, a secure connection, including encryption/decryption, in a VPN, means that the encryption is performed at the external client, and decryption is performed at the VPN server. Although the examiner believes Kramer is more than sufficient for this teaching, he has included Halme to explicitly state this.

The Appellant is correct that a WAP gateway typically converts a WTLS request, but this is not always the case. A dedicated public line may be used with a wireless client, and the WAP

conversion may take place at the entrance to the corporate network, along the lines of the present invention. Thus, although the appellant is correct about a typical WAP setup, the examiner asserts that a VPN connection to a corporate network does not need to use said typical method, and may use a method such as the examiner has suggested, and that which is taught by Kramer. Thus in the method taught by Kramer, the VPN server would receive WTLS data.

Examiner has interpreted “data center” with the broadest reasonable interpretation. Kramer teaches a private corporate network, that the examiner considers a data center. The VPN server is an apparatus coupled to a public network, that decrypts data, and forwards requests to the internal resources (servers). However, again, Halme has been included to explicitly teach a similar data center.

Appellant argues that Halme does not teach an apparatus to reside in a data center coupled between a public network and a server of the data center, and that converts SSL and WTLS to unencrypted data.

The examiner admits that Halme does not teach SSL or WTLS. What Halme does teach is an apparatus that is coupled between a public network and a server, where said apparatus decrypts data sent over a VPN tunnel, and forwards it to a server in the data center (Col 1 lines 20-35), (Col 3 lines 30-55 Fig 3). Halme thus supports Kramer, by explicitly teaching a VPN with encryption decryption at the VPN node, and forwarding to a server in the “data center” where the data center comprises a private/corporate network.

Appellant argues not suggestion or motivation is made by the examiner. The examiner asserts that all three references are of analogous arts in network communications, and security. Examiner also asserts that the strict TMS test the appellant is referring to has been changed to a flexible TMS/ common sense standard, via KSR v. Teleflex.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

11) Related Proceeding(s) Appendix

Copies of the court or Board decision(s) identified in the Related Appeals and Interferences section of this examiner's answer are provided herein.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Christopher J Brown/

Primary Examiner, Art Unit 2439

Art Unit: 2439

Conferees:

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439